DISTRIBUTION-BASED LOGISTICS OPERATIONS

LTC Carl W. Hunt

Introduction

Information assurance (IA) and logistics operations permeate all areas of the Army transformation. IA is critical to distribution-based logistics operations because timelines and pipelines for delivery of logistics packages are increasingly constrained by environmental factors that are rarely under direct Army control. Short timelines are critical to the success of OCONUS military operations, but they clearly challenge operational planners more than ever. The convergence of emerging logistics and information technologies, in-transit visibility systems, new players, and advanced delivery capabilities reflect more complexity than Army logisticians have previously encountered.

The U.S. Army Criminal Investigation Command (CID) is responsible for enforcing three critical factors involved in distribution-based logistics operations: IA, fraud deterrence, and logistics security (LOGSEC). The CID provides law enforcement and criminal investigative support for information assurance and pre- and in-transit delivery of logistics packages, including preconfigured loads. In fact, LOGSEC is a strategic mission for the CID. The command considers it a key force protection capability that it can uniquely offer to the Army.

Although responsible for only three of the factors that add to the complexity of modern logistics operations, the CID is modeling its role and interfaces into the entire LOGSEC knowledge-management process, understanding that criminal investigative support is critical to logistics operations throughout the logistics process. This article examines some initial intersections of the CID's roles and research in IA, knowledge management, and logistics security.

Because of the complexity of the logistics system and its information support systems, and the countless threats to these systems, a new approach by criminal investigators is required. The CID is conducting preliminary research into new areas of modeling and simulation, known as agent-based modeling. This research involves studying the intersections of critical nodes and their linkages to produce insights for those responsible for the direction of logistics and IA operations.

Initially directed at the criminal investigation domain, the CID has initiated research into knowledge-management support for advanced network intrusion defense and forensics capabilities for IA. Supported by the Office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts, the CID and the Krasnow Institute for Advanced Studies at George Mason University (GMU) are working jointly to model roles and actions of important players in the IA world.

Findings from this joint research will support logistics operations in at least two important ways. First, any improvement in IA will directly benefit LOGSEC and strengthen the role of the CID in supporting in-transit security of logistics packages. Second, in keeping with the extensibility of new agent-based modeling tools, insights gained from understanding networks of communication nodes will likely have significant application in logistics preparation and distribution. Research will be peripherally directed at the convergence of IA and LOGSEC, both in support of the CID's role in IA and LOGSEC as well as all logistics operations for the Army.

Agent-Based Modeling

Agent-Based Modeling (ABM) is an emerging modeling technology for enhancing inference about complex problems. ABM complements deduction and induction as a method of testing what American philosopher Charles S. Peirce called abductions (creative reasoning in uncertainty for which we have little or no probabilistic support). Abductive reasoning enhances the processes of discovery and incorporating theories and explanations about relationships for which we initially have only scant proof.

This new modeling technique encourages visualization of complex relationships and agent interaction. Agents are software manifestations of objects (animate or inanimate) used to represent the components of a problem domain. These agents are typically imbued with constraints (rules) to govern their behavior in an environment, and characteristics that may include movement, self-awareness, and processing capabilities such as learning and memory. Agents typically act on our behalf or sometimes on the behalf of themselves or others.

Using agent-based modeling, analysts and investigators can develop novel strategies for protecting and delivering both information-rich logistics support and the more conventional physical objects such as "beans and bullets." ABM supports transportation planning and operational deployment as well because complex scheduling problems lend themselves nicely to an agent-based modeling environment. (See agent-based modeling resources at **http://www.cna.org/isaac/** for

more background on these important new modeling techniques.)

Generally, ABM is an excellent starting point to uncover meaningful and often nonlinear relationships among diverse objects in circumstances where planners are not certain where to begin their planning and development efforts. While not explicitly incorporated into the Army acquisition and logistics community's modeling and broad-reaching simulation effort called Simulation and Modeling for Acquisition, Requirements and Training (SMART), ABM clearly has a role in both strategic and tactical applications of logistics operations.

Roles And Research

The CID applies distinct efforts toward protecting and enforcing Army information assurance and logistics operations. Two essential CID units in these efforts are components of the 701st Military Police (MP) Group headquartered at Fort Belvoir, VA. The Computer Crime Investigative Unit (CCIU) is the Army's leading IA enforcement agency and is responsible for investigating felony intrusions of all Army information technology assets. The Major Procurement Fraud Unit, also a 701st MP Group asset, currently investigates criminal activity associated with the production and delivery of Army materials from manufacturer to points of embarkation. Garrison and deployed CID elements take up LOGSEC responsibilities from the points of embarkation through theater delivery of logistics. Likewise, local and regional CID computer crime coordinators support the CID and CCIU in the IA arena.

The CID began its ABM research with the introduction of the Agent Based Evidence Marshaling (ABEM) model. This model visually reflects the results of interactions among all agents to which a complex crime is only partially visible. Through these interactions, relevant agents build time-space vectors of their existence from the time they were first involved in the crime (either as witnesses or supporting objects otherwise associated in the crime).

The agents share information and learn to infer the importance of other agents' time-space vectors to their own, producing a global visualization of the crime. This results in emergent, self-organized databases capable of producing and testing hypotheses about their existence in the overall environment of the crime. This work has been extended in projects supported by the Defense Advanced Research Projects Agency and the Office of the Secretary of Defense (OSD).

In the ABEM model, each agent has only incomplete local knowledge about the crime. By allowing these agents to interact and build a self-organizing database, the knowledge about the crime dynamically emerges in a time-space relationship. The agents communicate with each other by means of tuples (a message-passing schema). (See **http://www.msiac.dmso.mil/journal/hunt23.html** for more information about the ABEM model.)

In August 2001, the CID began collaborating with the Krasnow Institute for Advanced Studies at GMU and Bios Group Inc. to extend the ABEM work by building an agent-based model of network intrusions in support of an OSD advanced concept technology demonstration. This collaboration, known as Advanced Network Intrusion Defense, will involve studying the feasibility of using ABM. The CID-GMU collaboration will create agent-based representations of the major players in a network intrusion activity.

The objects and their interactions studied in this model include computer intruders (e.g., hackers); network assets (routers, switches, and host computers); computer users; law enforcement officials; and the legal/policy environment. A proposal under consideration is a scenario involving a logistics distribution event, further demonstrating the important intersections of IA and LOGSEC.

Future research in this area may also embrace agent-based modeling of fraud cases to study the complex relationships of various animate and inanimate objects associated with such crime. Such a model could aid individuals in visualizing the people, surroundings, equipment, and supporting documents as agents capable of interacting to produce novel behaviors. This will enhance discovery of important relationships. These future agents could interact on their own behalf to build associations that chart the environment of the crime, much as the ABEM model tracks relationships of witnesses to inanimate objects empowered to act on their own behalf.

Summary

The CID plays an important role in securing logistics distribution for the Army as well as enforcing federal laws that protect information assurance. Because IA and LOGSEC are integral components of successful distribution-based logistics operations, the CID's force protection contributions are essential to those emerging logistics processes envisioned in the Army transformation. The CID is studying the role of innovative modeling and simulation support to IA and LOGSEC. This initial research is expected to support the transformation of Army logistics operations, thus resulting in effective and reliable tools for all commanders to enhance their force-protection capabilities.

LTC CARL W. HUNT is Commander of the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit. He received his Ph.D. in information technology from George Mason University and can be contacted at ***carl.hunt@us.army.mil****.*

USARPAC KNOWLEDGE MANAGEMENT EFFORTS

Libby Christensen and Maria Sadd

Introduction

The abundance of knowledge-management (KM) tools coming onto the market provide structure and knowledge repositories for identifying, organizing, and disseminating information. However, KM is not only about the tools. In fact, individuals who rely solely on the tools may not be successful in implementing KM. Furthermore, KM tools frequently require a substantial upfront investment as well as costly and recurring maintenance. Not only is there more to knowledge management than just the tools, but there are also less costly ways to implement an effective KM Program.

HQ, U.S. Army, Pacific (USARPAC) implemented a highly effective KM program that is transforming USARPAC into a knowledge-based organization at minimal cost. Our strategy emphasizes business process and tool reuse, which increases effectiveness by using what is familiar, and contributes to minimizing cost by reducing the need for new tools and training.

One KM challenge facing USARPAC is the organization's dispersed nature, which today spans 16 time zones and consists of Active and Reserve Army forces in Japan, Hawaii, and Alaska, and Reserve forces in Washington, Guam, and American Samoa. Therefore, while our current KM effort is focused at USARPAC, it is designed to enable knowledge sharing with major subordinate commands (MSCs) and Army KM and other Service components.

USARPAC Approach

KM is a critical enabler as we undergo the Army transformation. USARPAC defined the return on investment for KM as improved product quality and workplace morale. Our goal is to "empower the USARPAC workforce to actively leverage our Intellectual Capital as a critical enabler for Army Transformation and Joint Vision 2020, and to become an effective Knowledge-based organization."

Recognizing that KM is overwhelmingly more about people and processes than about technology, we have focused our program on business processes, particularly those that support our core priority missions. We contracted with the U.S. Army Information Systems Engineering Command (USAISEC) KM group to facilitate a series of focused meetings, or charrettes. To achieve KM buy-in, we included staff members from all levels and functional areas in defining the top program priorities and solicited input from senior leaders, subject matter experts, action officers, information officers, system administrators, and administrative personnel. The charrettes gathered input on the current and desired state of knowledge sharing in USARPAC by posing questions on knowledge culture, sources, accessibility, and responsibility, as well as tools, policies, business practices, and issues. Participants were invited to define how to transition to a learning organization. Through discussion and consolidation, we identified seven top priorities that included issues that both apply to the KM Program and that will effectively complement and augment our KM initiative.

USARPAC KM Implementation

USARPAC's KM implementation is an ongoing process that includes incorporating knowledge management into new and existing programs, modifying business practices to improve efficiency and increase process reuse, and deploying additional tools to support business practices. A significant key to our success is the strong support from our senior leaders.

To incorporate KM into the organization structure, USAISEC analyzed the network information infrastructure to ensure that it would support the required information flow and ensure that planned upgrades would continue to support KM implementation. The analysis addressed the local infrastructure and wide area networks. This effort included the Common User Installation Transport Network upgrades to ensure that our architecture was optimized to support the KM implementation and information flow. The analysis took a total systems approach, including the DOD Information Technology Security Certification and Accreditation Process, training, and user support.

The charrettes helped USARPAC knowledge workers identify those practices and processes with the most impact on our core priority missions. Key processes included resource management, strategic planning, suspense tracking, and training. A review of these key processes revealed redundancies, inefficiencies, and opportunities for process reuse. Many of the processes were streamlined and improved by using automation and by turning tacit knowledge into guidelines and checklists for routine and repetitive tasks.

After evaluating the business process requirements and achieving widespread buy-in, we identified KM tools suited to our needs. Some of our tool selection criteria include low cost, user friendliness, portability, and reusability. Because workflow processes are a large part of KM improvements, the Workflow Management System (WMS) tool, based on Microsoft Outlook, was selected to meet our requirements. In fact, the Office 2000 suite, which minimizes our acquisition costs and training requirements, is already our standard. To implement and customize individual views of the USARPAC portal, we selected Microsoft Digital Dashboard 2 portal framework, in compliance with the Defense Collaborative Tool Suite.

USARPAC KM is an evolving process that can be modified based on changing roles and missions. Our Information Management (IM) Panel is also evolving to support KM imple-